ABSTRACT

The invention concerns a tamper-resistant electronic circuit configured for implementation in a device. The electronic circuit securely implements and utilizes device-specific security data during operation in the device, and is basically provided with a tamper-resistantly stored secret not accessible over an external circuit interface. The electronic circuit is also provided with functionality for performing cryptographic processing at least partly in response to the stored secret to generate an instance of device-specific security data that is internally confined within said electronic circuit during usage of the device. The electronic circuit is further configured for performing one or more security-related operations or algorithms in response to the internally confined device-specific security data. In this way, secure implementation and utilization device-specific security data for security purposes can be effectively accomplished. The security is uncompromised since the stored secret is never available outside the electronic circuit, and the device-specific security data is internally confined within the circuit during usage or operation of the device.